

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-87458

(P2003-87458A)

(43) 公開日 平成15年3月20日 (2003.3.20)

(51) Int. Cl.	識別記号	F I	テ-リ-ト (参考)
H 0 4 N 1/00	1 0 7	H 0 4 N 1/00	C 2 C 0 6 1
B 4 1 J 29/00		G 0 6 F 3/12	1 0 7 Z 5 B 0 2 1
G 0 6 F 3/12		B 4 1 J 29/00	K 5 C 0 6 2
			Z

審査請求 未請求 請求項の数 4 O L (全 14 頁)

(21) 出願番号 特願2001-281218(P2001-281218)

(22) 出願日 平成13年9月17日 (2001.9.17)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 田中 友輝

大阪府大阪市阿倍野区長池町22番22号

シャープ株式会社内

(74) 代理人 110600062

特許業務法人第一国際特許事務所

P ターム (参考) 20061 AP01 AP07 CL08 CL10

58021 A401 NN18

50062 A405 A406 A435 A806 A822

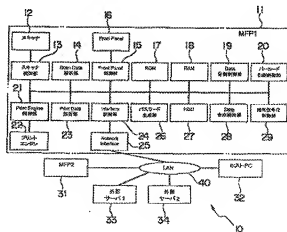
A842 AC24 A807 AP12 BA00

(54) 【発明の名称】 機密保護機能付き画像形成システム

(57) 【要約】

【課題】 印刷データの機密保護をより高めた機密保護機能付き画像形成システムの提供。

【解決手段】 機密保護機能付き画像形成システム 10 は、スキャナ 12 と、プリントデータ解析部 23 と、HDD 27 と、ネットワークインタフェース 25 と、インタフェース制御部 24 と、バーコード印刷制御部 20 と、スキャンデータ解析部 14 を有する。インタフェース制御部 24 とネットワークインタフェース 25 を用いて情報を外部ファイルサーバ 33、34 或いは HDD 27 に格納する。スキャンデータ解析部 14 により得たデータから外部ファイルサーバ 33、34 或いは HDD 27 中の印刷データを読み出して実際のジョブの印刷を行う。



## 【特許請求の範囲】

【請求項 1】 画像読み取り機能を備えた画像形成システムにおいて、

画像の読み取りを行う画像読み取り手段と、受信データから印刷ジョブの機密保護要求を判断する機密保護要求判断手段と、印刷データを記憶する記憶手段と、ネットワークへの接続可能とするネットワークインタフェース手段と、上記ネットワークインタフェース手段を介して外部ファイルサーバあるいは上記記憶手段に情報を格納する印刷データ格納手段と、上記外部ファイルサーバあるいは上記記憶手段に格納された各ジョブのデータが存在する場所を識別情報として印刷する識別情報イメージ生成手段と、上記識別情報イメージ生成手段によって生成された印刷物を読み取りその内容を解析する識別情報イメージ解析手段とを有し、上記機密保護要求判断手段により機密保護要求がなされていると判断した場合に、上記印刷データ格納手段と上記ネットワークインタフェース手段を用いて印刷に必要な情報を全て上記外部ファイルサーバあるいは上記記憶手段に格納し、上記外部ファイルサーバあるいは上記記憶手段のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトを上記識別情報イメージ生成手段により作成し、上記識別情報のプリントアウトを上記画像読み取り手段により読み取り、上記識別情報イメージ解析手段により解析し、上記識別情報イメージ解析手段によって得たデータから上記外部ファイルサーバあるいは上記記憶手段中の印刷データを読み出して実際のジョブの印刷を行うことを特徴とする機密保護機能付き画像形成システム。

【請求項 2】 上記実際のジョブの印刷に必要な情報を複数の分割するデータ分割手段と、分割された情報を再構成するデータ再構成手段とを有し、上記データ分割手段により分割されたデータを複数の外部ファイルサーバあるいは上記記憶手段からランダムに選択された 1 つの外部ファイルサーバあるいは記憶手段にそれぞれ格納し、その格納場所及びデータの順序または位置情報を識別情報として印刷し、上記識別情報のプリントアウトを読み込むことによって分割されたデータのそれぞれを順次読み出して再構成し、元データの印刷を可能とした請求項 1 に記載の機密保護機能付き画像形成システム。

【請求項 3】 パスワードを自動的に生成するパスワード自動生成手段と、印刷する識別情報シートに対して識別情報シート番号を付与する識別情報シート番号付与手段と、上記パスワード自動生成手段により生成されたパスワードと識別情報シート番号を機密保護要求が施されたジョブを発行したホスト P C に通知するパスワード通知手段と、パスワードを入力するパスワード入力手段とを有し、上記識別情報シート印刷時に上記識別情報シート番号付与手段によって識別情報シート番号を付与すると共に、上記パスワード通知手段によってジョブ発行元の上記ホスト P C に識別情報シート番号と上記パスワ

ード自動生成手段によって生成されたパスワードを通知し、実際のジョブの印刷時に上記パスワード入力手段によるパスワードの入力を要求するようにした請求項 1 に記載の機密保護機能付き画像形成システム。

【請求項 4】 データの暗号化手段と復号化手段を有し、機密保護要求されたジョブの格納時には、パスワード自動生成手段により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに上記暗号化手段により暗号化を行い、機密保護要求されて格納されたデータの印刷時には、パスワード入力手段により入力されたパスワードをキーとして識別情報生成用データ及び実際のジョブの印刷データの復号化を行うようにした請求項 3 に記載の機密保護機能付き画像形成システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、機密保護機能付き画像形成システムに関し、特に、印刷データの機密保護をより高めることと、ネットワーク上に接続された同様の機能を備えた任意の機器から機密保護された情報を取り出すことを可能にすることを主目的としたものである。

## 【0002】

【従来の技術】 近年、画像形成装置の Multi Function 化が進み、複写機能と、プリンタ機能と、スキャン機能と、ファクシミリ機能が 1 台で実現されてきており、さらに、ネットワークへの接続が進んでいるが、印刷データは MFP (Multi Function Print) 機器内で一旦格納された後に印刷されるため、いつ出力されるのかが不明である。さらに、ネットワーク等から送られる印刷データは、印刷要求者が離れていくことが多く、機密文書を印刷した場合に、印刷結果を他人に見られることなく入手するために、MFP 機器の前で自分の印刷が始まってから完了するまで待ち続ける必要があった。

【0003】 このような問題点を解決するものとして、特開平 9-251358 号公報に開示されたように、プリントアウトデータに識別コードを付加し、ユーザーがプリンタ部に同一識別コードを入力した時にのみプリントアウトを可能とする第 1 の方法や、ユーザーがプリンタ部に識別コードを入力する代わりに識別コードを書き込んだ磁気カードをリーダー部に読み取らせ、その識別コードがプリントアウトデータに含まれる識別コードと一致した時にのみプリントアウトを可能とする第 2 の方法もあった。

【0004】 さらに、特開平 11-334158 号公報に開示されたように、ユーザー識別コードを記載したカードを各ユーザーに携帯させ、これを画像読み取り手段に読み取らせ、このカードに記載されているユーザー識別コードがプリントアウトデータに含まれる識別コー

ドと一致した時のみプリントアウトを可能とする第3の方法もあった。

【0005】

【発明が解決しようとする課題】しかしながら、上記特開平9-251358号公報及び特開平11-334158号公報に開示された方法では、いずれも最終的に印刷される印刷データの格納先が当該機器内のメモリであることは明らかであり、当該機器内のメモリをアクセスすることにより、機密性は脆弱なものとなる。また、印刷物を任意の場所から取得することができず、不便であった。

【0006】本発明は、上記従来の問題点に鑑み、印刷データの格納先を他人に漏らすことなく、安全に格納でき、任意のタイミングで任意の場所からプリントアウトを得ることができ、印刷ジョブの機密保護性を向上させ、さらに、ネットワーク上に接続された同様の機能を持つ任意の機械からでも実際のジョブの印刷を可能とした機密保護機能付き画像形成システムを提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の機密保護機能付き画像形成システムは、画像読み取り機能を備えた画像形成システムにおいて、画像の読み取りを行う画像読み取り手段と、受信データから印刷ジョブの機密保護要求を判断する機密保護要求判断手段と、印刷データを記憶する記憶手段と、ネットワークへの接続可能とするネットワークインタフェース手段と、上記ネットワークインタフェース手段を介して外部のファイルサーバ或いは上記記憶手段に情報を格納する印刷データ格納手段と、上記外部のファイルサーバ或いは上記記憶手段に格納された各ジョブのデータが存在する場所を識別情報として印刷する識別情報イメージ生成手段と、上記識別情報イメージ生成手段によって生成された印刷物を読み取りその内容を解析する識別情報イメージ解析手段とを有し、上記機密保護要求判断手段により機密保護要求がなされていると判断した場合に、上記印刷データ格納手段と上記ネットワークインタフェース手段を用いて印刷に必要な情報を全て上記外部のファイルサーバ或いは上記記憶手段に格納し、上記外部のファイルサーバ或いは上記記憶手段のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトを上記識別情報イメージ生成手段により作成し、上記識別情報のプリントアウトを上記画像読み取り手段により読み取り、上記識別情報イメージ解析手段により解析し、上記識別情報イメージ解析手段によって得たデータから上記外部のファイルサーバ或いは上記記憶手段中の印刷データを読み出して実際のジョブの印刷を行うことを特徴とするものである。

【0008】本発明の機密保護機能付き画像形成システムは、上記実際のジョブの印刷に必要な情報を複数に分割するデータ分割手段と、分割された情報を再構成する

データ再構成手段とを有し、上記データ分割手段により分割されたデータを複数の外部ファイルサーバ或いは上記記憶手段からランダムに選択された1つの外部ファイルサーバ或いは記憶手段にそれぞれ格納し、その格納場所及びデータの順序或いは位置情報を識別情報として印刷し、上記識別情報のプリントアウトを読み込むことにより分割されたデータのそれぞれを順次読み出して再構成し、元データの印刷を可能としたものである。

【0009】本発明の機密保護機能付き画像形成システムは、パスワードを自動的に生成するパスワード自動生成手段と、印刷する識別情報シートに対して識別情報シート番号を付与する識別情報シート番号付与手段と、上記パスワード自動生成手段により生成されたパスワードと識別情報シート番号を機密保護要求が施されたジョブを発行したホストPCに通知するパスワード通知手段と、パスワードを入力するパスワード入力手段とを有し、上記識別情報シート印刷時に上記識別情報シート番号付与手段によって識別情報シート番号を付与すると共に、上記パスワード通知手段によってジョブ発行元の上記ホストPCに識別情報シート番号と上記パスワード自動生成手段によって生成されたパスワードを通知し、実際のジョブの印刷時に上記パスワード入力手段によるパスワードの入力を要求するようにしたものである。

【0010】本発明の機密保護機能付き画像形成システムは、データの暗号化手段と復号化手段を有し、機密保護要求されたジョブの格納時には、パスワード自動生成手段により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに上記暗号化手段により暗号化を行い、機密保護要求されて格納されたデータの印刷時には、パスワード入力手段により入力されたパスワードをキーとして識別情報生成用データ及び実際のジョブの印刷データの復号化を行うようにしたものである。

【0011】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。図1は本発明の実施の形態における機密保護機能付き画像形成システムを示すブロック図である。本発明の機密保護機能付き画像形成システム10は、図1に示すように、MFP (Multi Function Print) 機器11が画像の読み取りを行う画像読み取り手段となるスキャナ12と、受信データから印刷ジョブの機密保護要求を判断する機密保護要求判断手段となるプリントデータ解析部23と、印刷データを記憶する記憶手段となるハードディスクドライブ (Hard Disk Drive; HDD) 27と、ローカルエリアネットワーク (Local Area Network; LAN) 40への接続可能とするネットワークインタフェース手段となるネットワークインタフェース25と、ネットワークインタフェース25を介して外部ファイルサーバ33、34或いはハードデ

ィスクドライブ（以下HDDという）27に情報を格納する印刷データ格納手段となるインタフェース制御部24と、外部ファイルサーバ33、34或いはHDD27に格納された各ジョブのデータが存在する場所を識別情報として印刷する識別情報イメージ生成手段となるバーコード印刷制御部20と、バーコード印刷制御部20によって生成された印刷物となる識別情報シートを読み取りその内容を解析する識別情報イメージ解析手段となるスキャンデータ解析部14とを有し、プリントデータ解析部23により機密保護要求がなされていると判断した場合に、インタフェース制御部24とネットワークインタフェース25を用いて印刷に必要な情報を全て外部ファイルサーバ33、34或いはHDD27に格納し、外部ファイルサーバ33、34或いはHDD27のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトをバーコード印刷制御部20により作成し、識別情報のプリントアウトをスキャナ12により読み取り、スキャンデータ解析部14により解析し、スキャンデータ解析部14によって得たデータから外部ファイルサーバ33、34或いはHDD27中の印刷データを読み出して実際のジョブの印刷を行うようになっている。

【0012】本発明の機密保護機能付き画像形成システム10は、図1に示すように、MFP機器11が実際のジョブの印刷に必要な情報を複数の分割するデータ分割手段となるデータ分割制御部19と、分割された情報を再構成するデータ再構成手段となるデータ合成制御部28とを有し、データ分割制御部19により分割されたデータを複数の外部ファイルサーバ33、34或いはHDD27からランダムに選択された1つの外部ファイルサーバ33、34或いはHDD27にそれぞれ格納し、その格納場所及びデータの順序或いは位置情報を識別情報として印刷し、識別情報のプリントアウトを読み込むことによって分割されたデータのそれぞれを順次読み出して再構成し、元データの印刷を可能とてある。

【0013】本発明の機密保護機能付き画像形成システム10は、図1に示すように、パスワードを自動的に生成するパスワード自動生成手段となるパスワード生成部26と、印刷する識別情報シートであるバーコードシートに対して識別情報シート番号を付与する識別情報シート番号付与手段となるプリントエンジン22と、パスワード生成部26により生成されたパスワードと識別情報シート番号を機密保護要求が施されたジョブを発行したホストPC32に通知するパスワード通知手段となるフロントパネル制御部15と、パスワードを入力するパスワード入力手段となるフロントパネル16とを有し、上記識別情報シート印刷時にプリントエンジン22によって識別情報シート番号を付与すると共に、フロントパネル制御部15によってジョブ発行元のホストPC32に識別情報シート番号とパスワード生成部26によって生

成されたパスワードを通知し、実際のジョブの印刷時にフロントパネル16によるパスワードの入力を要求するようになっている。

【0014】本発明の機密保護機能付き画像形成システム10は、図1に示すように、MFP機器11がデータの暗号化手段と復号化手段となる暗号番号化制御部29を有し、機密保護要求されたジョブの格納時には、パスワード生成部26により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに暗号番号化制御部29により暗号化を行い、機密保護要求されて格納されたデータの印刷時には、フロントパネル16により入力されたパスワードをキーとして識別情報生成用データ及び実際のジョブの印刷データの復号化を行うようになっている。

【0015】本発明の機密保護機能付き画像形成システム10は、図1に示すように、MFP機器11とMFP機器31とホストPC32と外部ファイルサーバ33と外部ファイルサーバ34とがローカルエリアネットワーク（以下LANという）40を介して接続され、MFP機器11はスキャナ12と、スキャナ制御部13と、スキャンデータ解析部14と、フロントパネル制御部15と、フロントパネル16と、ROM（Read Only Memory）17と、RAM（Random Access Memory）18と、データ分割制御部19と、バーコード印刷制御部20と、プリントエンジン制御部21と、プリントエンジン22と、プリントデータ解析部23と、インタフェース制御部24と、ネットワークインタフェース25と、パスワード生成部26と、HDD27と、データ合成制御部28と、暗号番号化制御部29を有している。

【0016】11は本発明の機密保護機能付き画像形成システム10の中心となるMFP機器であり、MFP機器11はスキャナ12、スキャナ制御部13、スキャンデータ解析部14、フロントパネル制御部15、フロントパネル16、ROM17、RAM18、データ分割制御部19、バーコード印刷制御部20、プリントエンジン制御部21、プリントエンジン22、プリントデータ解析部23、インタフェース制御部24、ネットワークインタフェース25、パスワード生成部26、HDD27、データ合成制御部28、暗号番号化制御部29の要素を有する。

【0017】12はMFP機器11のうち画像の読み取りを行うスキャナである。

【0018】13はスキャナ12の制御を行うスキャナ制御部である。

【0019】14はバーコードのデータ解析及び入力画像におけるチェックボックスのチェックの有無の判断を行うスキャンデータ解析部であり、スキャナ12がスキャナ制御部13により制御されて読み取った画像データを解析する部分である。

【0020】15はフロントパネル16の制御を行うフロントパネル制御部である。

【0021】16はMF P機器11のユーザーインタフェースを担うフロントパネルである。

【0022】17はMF P機器11の全体の制御を行うプログラム及びバーコードフォントを含むフォントデータを格納するためのROMである。

【0023】18はMF P機器11の動作中の中間データやイメージデータ用のエリア及びワークエリアとして用いられるRAMである。

【0024】19はRAM18上に展開されたイメージデータを分割処理するデータ分割制御部であり、イメージデータの分割制御をつかさどる部分である。このデータ分割制御部19は、自ら分割制御したイメージデータを、インタフェース制御部24により制御されるネットワークインタフェース25を介して接続された他のMF P機器31を含む外部ファイルサーバ33、34に格納する処理を行う。

【0025】該格納場所に関する情報はRAM18上に各々記憶され、これをパスワード生成部26によって生成されるパスワードをキーとして暗号復号化制御部29にて暗号化され、当該暗号化されたデータをバーコード印刷制御部20にてバーコードイメージデータに変換され、RAM18上に展開される。この展開されたデータは、プリントエンジン制御部21によってプリントエンジン22に送信され、プリントエンジン22により印刷される。

【0026】20はバーコード印刷制御部であり、RAM18上に記憶されているデータをROM17内に格納されているバーコードフォントデータを用いてバーコードイメージデータとしてRAM18上に展開する部分である。該バーコードイメージデータはプリントエンジン制御部21を介してプリントエンジン22にて印刷処理される。

【0027】21はプリントエンジン22の制御を行うプリントエンジン制御部であり、実際の印刷の際には、プリントデータ解析部23、バーコード印刷制御部20或いはデータ合成制御部28により作成され、RAM18上にイメージデータとして展開されたデータをプリントエンジン22に送信することによってプリント処理の制御を行う部分である。

【0028】22は実際の印刷処理を行うプリントエンジンである。

【0029】23はプリントデータ解析部であり、MF P機器11に対して、インタフェース制御部24によって制御されるネットワークインタフェース25を介して、LAN40に接続されたホストPC32から送信される印刷データを解析し、イメージデータに展開する部分である。このイメージデータに展開する部分において、プリントデータ解析部23は機密保護要求の判断も

行う。

【0030】24はインタフェース制御部であり、ネットワークインタフェース25の制御を行う部分である。このインタフェース制御部24により、ネットワークインタフェース25を介して、LAN40に接続されたホストPC32からの印刷データの受信制御、或いは、同じくLAN40に接続された各外部ファイルサーバ33、34や他のMF P機器31へのデータ送信制御、及び、これからのデータ取得制御、同じくLAN40に接続されたホストPC32へのパスワード等の情報送信制御を行うようになっている。

【0031】25はMF P機器11のLAN40への接続を可能とするためのネットワークインタフェースである。

【0032】26はパスワード生成部であり、プリントデータ解析部23において機密保護要求がなされていると判断されたジョブを発行したホストPC32に対して、実際のジョブデータ印刷のためのパスワードを生成する部分である。

【0033】パスワード生成部26で生成されたパスワードは、インタフェース制御部24によって制御されるネットワークインタフェース25を介して該ジョブを発行したホストPC32に対してパスワードを通知する。また、このパスワードは、暗号復号化制御部29においてデータの暗号化を行う時にキーとして用いられる。

【0034】27はHDDであり、各ジョブのデータや他のMF P機器31から格納要求されたデータを保持するための記憶手段である。このHDD27を用いて、このMF P機器11はファイルサーバとして動作することも可能となる。

【0035】28はイメージデータの合成制御を行うデータ合成制御部であり、上記データ分割制御部19にて分割処理され、パスワード生成部26により生成されたパスワードをキーとして暗号復号化制御部29において暗号化されたデータを元のデータに合成し、RAM18にイメージデータとして展開する制御を行う部分である。

【0036】この合成に必要な分割されたイメージの格納場所等の情報は、スキャナ12によって読み取られたバーコードイメージをスキャンデータ解析部14にて解析処理し、フロントパネル16から入力されたパスワードをキーとして、暗号復号化制御部29にて復号化されることによって得られる。復号化することによって得られたこれらの情報が無効な場合、フロントパネル制御部15を介してフロントパネル16上にエラーメッセージを表示する。

【0037】また、RAM18上に展開されたイメージデータは、プリントエンジン制御部21を介してプリントエンジン22に送信されて印刷処理される。

【0038】29は暗号復号化制御部であり、データ分

割制御部 19 において分割されて外部ファイルサーバ 33、34 等に送信されたイメージデータの所在や位置情報等の各種情報及びデータ分割制御部 19 にて分割されたイメージデータを、パスワード生成部 26 によって生成されたパスワードをキーとした暗号化処理を行い、処理後のデータはバーコード印刷制御部 20 に渡される。

【0039】また、スキャンデータ解析部 14 によってバーコード情報から電子情報に変換されたデータ及びこれら情報を用いて外部ファイルサーバ 33、34 や他の MFP 機器 31 から取得した暗号化済みのイメージデータの一部を、フロントパネル 16 から入力されたパスワード情報をフロントパネル制御部 15 から受け取り、これをキーとして復号化処理を行い、処理後のデータはデータ合成制御部 28 に渡される。

【0040】以上で、本発明の中心となる MFP 機器 11 に内蔵されるブロックである。

【0041】40 は LAN であり、複数の情報機器を接続して任意の機器間でデータ交換を可能にする。

【0042】LAN 40 には、図 1 に示すように、MFP 機器 11 と、MFP 機器 31 と、文書作成／編集を行うホスト PC 32 と、外部ファイルサーバ 33、34 がそれぞれ接続されている。

【0043】MFP 機器 11、31 は、それぞれ印刷機器・画像読み取り機器として動作するだけでなく、ファイルサーバとしても動作可能とすることができる。そのため、自分自身も本発明に記述されたファイルサーバとして動作することができる。

【0044】図 2 は本発明の機密保護機能付き画像形成システムに係わる受信ジョブ印刷処理の処理フロー図である。まず、印刷ジョブが機密保護機能付き画像形成システム 10 のホスト PC 32 より MFP 機器 11 に送信された時に、MFP 機器 11 のプリントデータ解析部 23 において印刷データの解析を行い、機密保護印刷 (Secure Print) 要求があるかを判断 (ステップ 101) する。

【0045】ステップ 101 において、機密保護印刷 (Secure Print) 要求があると判断された場合は、機密保護印刷フラグ (Secure Print Flag) を ON (ステップ 102) する。

【0046】ステップ 101 において、機密保護印刷 (Secure Print) 要求がないと判断された場合は、MFP 機器 11 のプリントデータ解析部 23 において印刷データの解析 (ステップ 103) を続けて行い、次いで、1 ページ分のイメージデータの生成 (ステップ 104) を行い、このイメージデータを MFP 機器 11 の RAM 18 に展開する。

【0047】ステップ 104 において、1 ページ分のイメージデータの生成が完了した後、機密保護印刷フラグが ON されているかを判断 (ステップ 105) する。

【0048】ステップ 105 において、機密保護印刷フラグが ON されていると判断された場合は、MFP 機器 11 のパスワード生成部 26 においてパスワードの生成 (ステップ 106) を行い、次いで、ステップ 104 において MFP 機器 11 の RAM 18 に展開されたイメージデータを、MFP 機器 11 のデータ分割制御部 19 においてイメージデータの分割処理 (ステップ 107) を行う。

【0049】さらに、ステップ 107 にて得られた分割済みのイメージデータを、MFP 機器 11 の暗号復号化制御部 29 において、ステップ 106 にて得られたパスワードをキーとした暗号化処理を行い、処理済みのデータを LAN 40 を介して MFP 機器 11 に接続された他の MFP 機器 31 や外部ファイルサーバ 33、34 にファイルとして送信して保持 (ステップ 108) させる。

【0050】この時、ステップ 107 にて分割したイメージデータの位置情報やページ情報、及び、ステップ 108 にて送信した送信先のサーバアドレスやファイル名等の情報を、MFP 機器 11 の RAM 18 に保持蓄積する。

【0051】ステップ 105 において、機密保護印刷フラグが OFF されていると判断された場合には、このページの通常印刷処理 (ステップ 109) を行い、次いで、通常印刷処理がジョブエンドであるかを判断 (ステップ 110) する。

【0052】ステップ 110 において、通常印刷処理がジョブエンドでない場合は、ステップ 103 に戻り、上記ページの通常印刷処理をジョブエンドまで実行する。

【0053】ステップ 110 において、通常印刷処理がジョブエンドである場合は、再度機密保護印刷フラグが ON されているかを判断 (ステップ 111) する。

【0054】ステップ 111 において、機密保護印刷フラグが ON されていると判断された場合には、ステップ 108 において保持蓄積した各種情報を、ステップ 106 にて得られたパスワードをキーとして、MFP 機器 11 の暗号復号化制御部 29 において暗号化し、この暗号化された情報を MFP 機器 11 の ROM 17 に格納されたバーコードフロントデータを用いて、MFP 機器 11 のバーコード印刷制御部 20 にてバーコードイメージデータを生成 (ステップ 112) する。

【0055】次いで、ステップ 112 において生成されたバーコードイメージデータを、MFP 機器 11 のプリントエンジン制御部 21 を介して MFP 機器 11 のプリントエンジン 22 に転送し、バーコードイメージデータの印刷処理 (ステップ 113) を行う。

【0056】次いで、ステップ 106 にて得られたパスワードを、LAN 40 を介してこの MFP 機器 11 と接続され、現在処理を行っているジョブの発行元であるホスト PC 32 に対して送信 (ステップ 114) し、パスワードとステップ 113 において印刷されたバーコード

シートに記載されるバーコードシート番号をユーザーに通知し、次いで、機密保護印刷プラグをOFF（ステップ115）にし、その後、現在のジョブを完了し、次のジョブに備える。

【0057】ステップ111において、機密保護印刷プラグがOFFされていると判断された場合には、何も行わずに現在のジョブを完了し、次のジョブに備える。以上が、図2の受信ジョブ印刷処理の処理フローの流れである。

【0058】図3は図1のMFP機器11に機密保持要求がなされた時に印刷されるバーコードシートの一例を示す図である。このバーコードシート50には、図3に示すように、タイトル51と、バーコードシート番号52と、バーコード53と、印刷後にデータを保存しておくか否かを指示するチェックボックス54と、印刷せずに保存されたデータを削除するか否かを指示するチェックボックス55が印刷されている。

【0059】特に、バーコードシート50に印刷されたバーコード53の部分には、このジョブに対する出力者IDやジョブID等のジョブ情報、各ページに対する用紙サイズや両面指示等の情報を含むページ情報、各ページにおいて分割された部品の位置情報とイメージデータの格納先情報が記述されている。

【0060】なお、このバーコードシートの一例においては、理解しやすいように各情報ブロック毎に実行処理が施されているが、実際にはその必要はない。

【0061】図4は図1のMFP機器11において、画像読み取り要求がなされた時のスキャンジョブ処理の処理フロー図である。まず、ユーザーが画像読み取りを指示した時、機密保護ジョブ印刷用のバーコード読み取りモードであるか否かを判断（ステップ201）し、ステップ201において、機密保護ジョブ印刷用のバーコード読み取りモードであると判断した場合には、MFP機器11のフロントパネル制御部15を介して、MFP機器11のフロントパネル16にパスワードの入力の要求を促すメッセージを表示（ステップ202）し、ユーザーによるパスワードの入力を待つ。

【0062】次いで、パスワードが入力されると、MFP機器11のスキャナ12において読み込んだイメージデータをMFP機器11のスキャナ制御部13から受け取り、MFP機器11のスキャンデータ解析部14においてバーコードデータの解析（ステップ203）を行い、次いで、バーコードデータの解析にエラーがあるか否かを判断（ステップ204）する。

【0063】ステップ204において、このバーコードデータの解析にエラーがあったと判断された場合には、読み込んだイメージデータが機密保護ジョブの再構成用バーコードイメージではないと判断し、MFP機器11のフロントパネル制御部15を介してMFP機器11のフロントパネル16にその旨を示すエラーメッセージを

表示（ステップ209）し、その後、ジョブを終了する。

【0064】ステップ204において、バーコードデータの解析にエラーがないと判断された場合には、MFP機器11の暗号復号化制御部29において、解析後のバーコードデータをステップ202において得たパスワードをキーとして復号化処理（ステップ205）を行い、次いで、復号化された情報から印刷要求されている機密保護ジョブにおいて分割／暗号化／保存された全てのデータの存在を検証（ステップ206）し、次いで、全データが存在するか否かを判断（ステップ207）する。

【0065】ステップ207において、全データの存在が確認された場合には、元イメージデータの復元処理（ステップ208）を行った後、このジョブを終了する。

【0066】ステップ207において、一部のデータが欠損していると判断した場合には、外部接続されている外部ファイルサーバ33、34に問題があると判断し、MFP機器11のフロントパネル制御部15を介してMFP機器11のフロントパネル16にその旨を示すエラーメッセージを表示（ステップ209）し、その後、ジョブを終了する。

【0067】ステップ207において、全てのデータが存在しない場合には、ステップ202において入力されたパスワードが不正なものであると判断し、MFP機器11のフロントパネル制御部15を介してMFP機器11のフロントパネル16にその旨を示すエラーメッセージを表示（ステップ209）し、その後、ジョブを終了する。

【0068】ステップ201において、機密保護ジョブ印刷用のバーコード読み取りモードでないとして判断した場合には、通常の画像読み取り処理であるスキャン処理（ステップ210）を行い、その後、ジョブを終了する。

【0069】図5は図4の元イメージデータの復元処理（ステップ208）の詳細な処理フロー図である。まず、MFP機器11のスキャンデータ解析部14において、読み取られた図3のバーコードシート50上で、印刷せずに保存されたデータを削除するか否かを指示する図3のチェックボックス55にユーザーによるチェックが施されているか否かを判断（ステップ301）し、ステップ301において、バーコードシート50のチェックボックス55にユーザーによるデータ削除のチェックが施されていると判断した場合には、図4の全データの存在検証処理（ステップ206）において得られた、読み取られたバーコードシート50に対応する図1の外部ファイルサーバ33、34上の全てのデータの削除処理（ステップ306）を行い、この処理を抜ける。

【0070】ステップ301において、バーコードシート50のチェックボックス55にユーザーによるデータ

削除のチェックが施されていないと判断した場合には、図4のバーコード解析処理(ステップ203)、図4のパスワードによる復号化処理(ステップ205)、図4の全データの存在検証処理(ステップ206)において得られた各種情報から、図1の外部ファイルサーバ33、34等に格納されたデータを順次取得(ステップ302)し、取得したデータを、図4のステップ202にて得られたパスワードをキーとしてMFP機器11の暗号復号化制御部29において復号化を行い、ページ単位でイメージデータの再構成(ステップ303)を行う。

【0071】再構成されたページデータは、MFP機器11のRAM18上に展開され、MFP機器11のプリントエンジン制御部21を介してMFP機器11のプリントエンジン22に転送され、印刷処理される。

【0072】次いで、ステップ303において印刷処理されたページにてジョブが完了しているか否かを判断(ステップ304)し、ステップ304において、ジョブが完了していると判断した場合には、MFP機器11の全データ解析部14において、読み取られた図3のバーコードシート50上で、印刷後にデータを保存しておくか否かを指示する図3のチェックボックス54にユーザーによるチェックが施されているか否かを判断(ステップ305)し、ステップ305において、バーコードシート50のチェックボックス54にユーザーによるデータ保存のチェックが施されていないと判断した場合には、図4の全データの存在検証処理(ステップ206)において得られた、読み取られたバーコードシート50に対応する図1の外部ファイルサーバ33、34上の全てのデータの削除処理(ステップ306)を行い、この処理を抜ける。

【0073】上記ステップ305において、バーコードシート50のチェックボックス54にユーザーによるデータ保存のチェックが施されていると判断した場合には、読み取られたバーコードシート50に対応する外部データの削除処理は行わず、この処理を抜ける。

【0074】このことによつて、同じバーコードシートとパスワードを用いて、ユーザーはこのジョブの再出力を行うことができる。

【0075】ステップ304において、ジョブが完了していないと判断した場合には、ステップ302に戻つて、次のページの処理を続ける。

【0076】なお、本発明の実施の形態では、特許請求の範囲にて記述された識別情報としてバーコードを用いては、特にバーコードに限定するものではなく、例えばは数字列や文字列を用いて識別を行うことも可能であることはいうまでもない。

【0077】

【発明の効果】以上に述べたように、本発明の機密保護機能付き画像形成システムによれば、機密保護要求判断手段により受信データから印刷ジョブの機密保護要求が

なされていると判断した場合に、印刷データ格納手段とネットワークインタフェース手段を用いて印刷に必要な情報を全て外部ファイルサーバ或いは記憶手段に格納することができ、外部ファイルサーバ或いは記憶手段のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトを識別情報イメージ生成手段により生成することができ、画像読み取り手段が識別情報イメージ生成手段により生成された識別情報のプリントアウトした印刷物を読み取ることで、その内容を識別情報イメージ解析手段により解析することができ、識別情報イメージ解析手段により得られたデータから外部ファイルサーバ或いは記憶手段中の印刷データを読み出して実際のジョブの印刷を行い、機密保護された印刷データを印刷するトリガとして、識別情報(例えばバーコード)の印刷物を用いているため、印刷システム単体ではその機密保護要求された印刷データそのものが存在することが漏れこともなく、印刷ジョブのより高い機密保護を行うことができる。また、ネットワークに接続された外部ファイルサーバもデータの保存が可能であるので、機密保護要求された印刷データの所在も隠蔽することができ、印刷ジョブのより高い機密保護性の向上が図れ、ネットワークに接続された同様の機能を持つ別のマシンからでも、実際のジョブの印刷を行うことが可能である。

【0078】本発明の機密保護機能付き画像形成システムによれば、機密保護を要求された印刷に対して、データ分割手段が実際のジョブの印刷に必要な情報を複数に分割するので、データ分割手段により分割されたデータを外部ファイルサーバ或いは記憶手段にばらばらに格納することができ、分割された一つ一つのデータは、その全体の部分でしかない。また、分割されたデータを再構成するに際し、その格納場所及びデータの順序或いは位置情報を識別情報として印刷し、識別情報のプリントアウトを読み込むことにより、データ再構成手段が分割されたデータのそれぞれを順次読み出して再構成するので、元データの印刷を行うことができ、別途出力した識別情報のプリントアウトした印刷物を用いるため、印刷ジョブのより高い機密保護性の向上を図ることができる。

【0079】本発明の機密保護機能付き画像形成システムによれば、識別情報シート印刷時に、識別情報シートに対して識別情報シート番号付手段により識別情報シート番号を付与することができ、パスワード自動生成手段がパスワードを自動的に生成するので、ジョブ発行元のホストPCにパスワード通知手段により識別情報シート番号とパスワードを通知することができ、実際のジョブの印刷時に、パスワードのパスワード入力手段による入力を要求するようにしたので、識別情報シートそのものを期待しない者に使用された場合には、実際のジョブの印刷のためには、パスワード入力手段にパスワードを入力しなければならず、印刷ジョブのより高い機密保護



性の向上を図ることができる。

【0080】本発明の機密保護機能付き画像形成システムによれば、機密保護要求されたジョブの格納時に、パスワード自動生成手段により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに暗号化手段により暗号化を行うことができ、識別情報シートを期待しない者により識別情報データが解析された場合にも、識別情報データは暗号化手段により暗号化されているため、パスワードを知らなければ、実際のジョブの印刷データの格納場所の機密を保つことができる。また、この実際のジョブの印刷データは同じく暗号化手段によって暗号化されているため、自分自身を含むファイルサーバ内のファイルを期待しない者が覗いても、意味のあるデータは存在しないため、印刷ジョブのより高い機密保護性の向上を図ることができる。さらに、機密保護要求されて格納されたデータの印刷時に、パスワード入力手段により入力されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データの復号化を行うことができる。

【図面の簡単な説明】

【図1】本発明の実施の形態における機密保護機能付き画像形成システムを示すブロック図。

【図2】本発明の機密保護機能付き画像形成システムに係る受信ジョブ印刷処理の処理フローチャート図。

【図3】図1のMFP機器に機密保持要求がなされた時に印刷されるバーコードシートの一例を示す図。

【図4】図1のMFP機器において画像読み取り要求がなされた時のスキャンジョブ処理の処理フローチャート図。

【図5】図4の元イメージデータの復元処理の詳細な処理フローチャート図。

【符号の説明】

10 機密保護機能付き画像形成システム

11 MFP機器

12 スキャナ

13 スキャナ制御部

14 スキャンデータ解析部

15 フロントパネル制御部

16 フロントパネル

17 ROM

18 RAM

19 データ分割制御部

20 バーコード印刷制御部

21 プリントエンジン制御部

22 プリントエンジン

23 プリントデータ解析部

24 インタフェース制御部

25 ネットワークインタフェース

26 パスワード生成部

27 ハードディスクドライブ

28 データ合成制御部

29 暗号復号化制御部

31 MFP機器

32 ホストPC

33 外部ファイルサーバ

34 外部ファイルサーバ

40 LAN

50 バーコードシート

51 タイトル

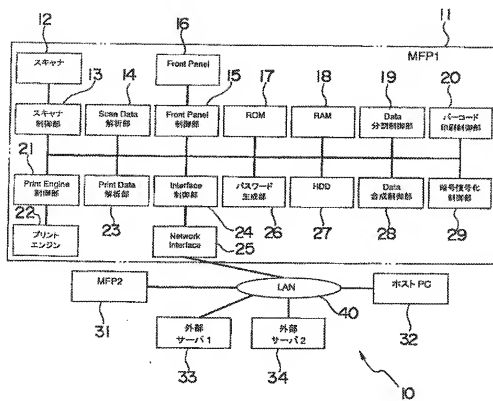
52 バーコードシート番号

53 バーコード

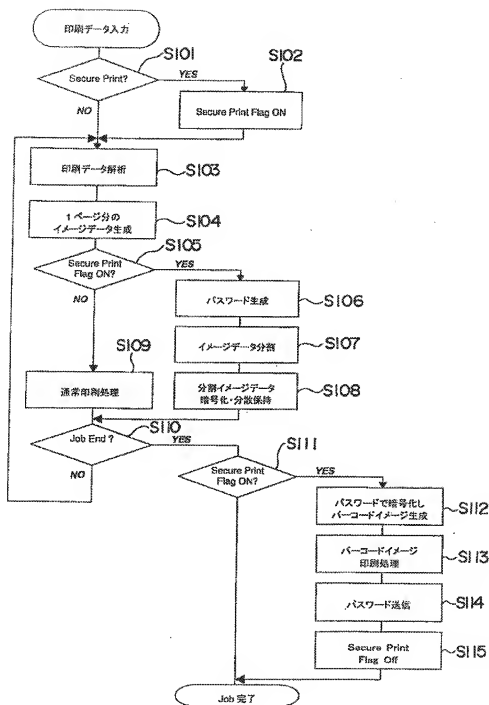
54 チェックボックス

55 チェックボックス

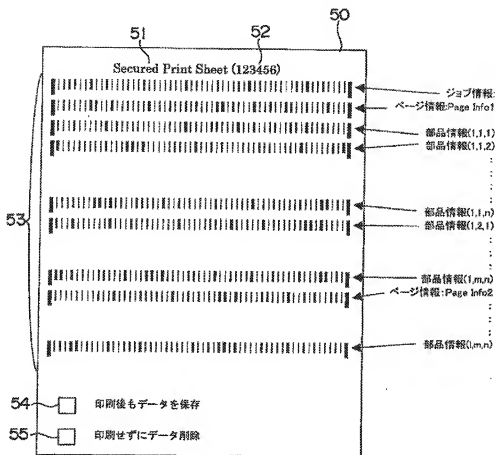
【図1】



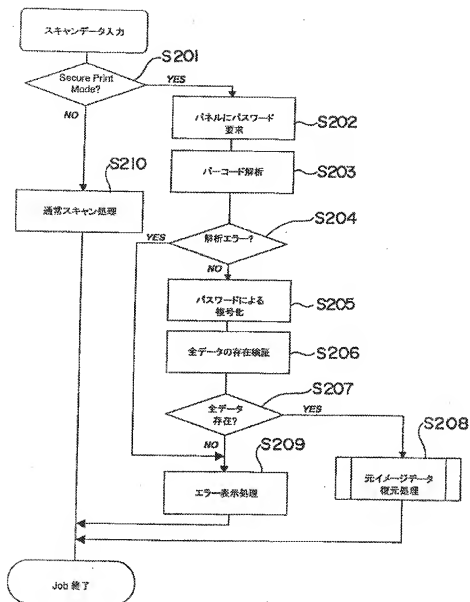
【図2】



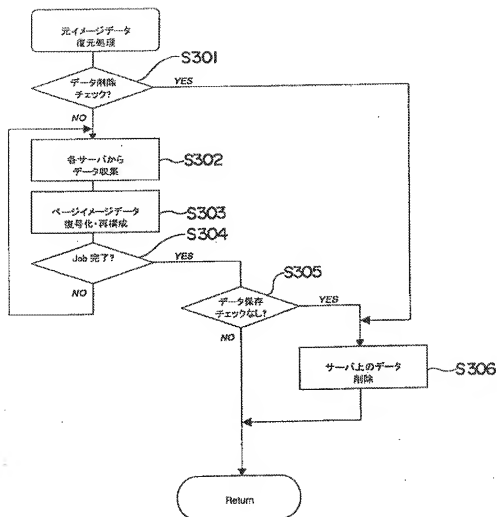
【図3】



【図4】



【図5】



## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087458

(43) Date of publication of application : 20.03.2003

(51)Int.Cl.

HO4N 1/00

B41J 29/00

G06F 3/12

(21)Application number : 2001-281218

(71)Applicant : SHARP CORP

(22)Date of filing : 17.09.2001

(72)Inventor : TANAKA TOMOKI

## (54) IMAGE FORMING SYSTEM WITH SECURITY PROTECTING FUNCTION

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an image forming system with a security protecting function that can enhance security protection of print data much more.

**SOLUTION:** The image forming system 10 with a security protecting function includes a scanner 12, a print data analysis section 23, an HDD 27, a network interface 25, an interface control section 24, a bar code print control section 20, and a scan data analysis section 14. Using the interface control section 24 and the network interface 25 stores information to external file servers 33, 34 or the HDD 27. Print data in the external file servers 33, 34 or the HDD 27 are read on the basis of the data obtained from the scan data analysis section 14 and used for the print of an actual job.

